Glossary

802.1Q — IEEE's open protocol specification for VLAN tagging.

abstract — A document that summarizes a longer, more detailed document.

Active Directory (AD) — Directory service developed by Microsoft.

active caching — Automatically update the pages in the cache from their Internet sources based on the number of requests for each page and the frequency at which it changes at the Internet source.

active-active configuration — A pair of devices that are configured in such a way that both are in service simultaneously and if either fails, the other will assume its role.

active-passive configuration — A pair of devices that are configured in such a way that only one is active and if it fails, the other will assume its role.

aggregate — A collection of somewhat similar items into one mass.

alert — In order to be made aware of the occurrence of a specified condition, you may create an alert, define the counters to be used and their thresholds, and define the update interval that you want. You may then define an action to be taken in the event an alert occurs.

Application layer — The seventh layer of the OSI reference model. This layer contains the services that give the user access to network resources. The user initiates client access through a user application, which in turn makes a request through the Application layer. Application layer services are often implemented through the use of an Application Programming Interface (API).

application portfolio — The list of applications that your client requires for inclusion.

Application Programming Interface (API) — A set of interfaces (now frequently in the form of an Object Model) that a software company publishes so that third parties can develop custom extensions to their software.

Application-layer packet filtering — Allows filtering of packets on a host-by-host basis.

Area Border Routers (ABR) — OSPF routers that connect their areas to a backbone area to which all OSPF areas connect.

asynchronous — A communications method that does not depend on strict time constraints and in which data streams can be broken by random intervals.

Asynchronous Transfer Mode (ATM) — A network technology that transfers data in cells or packets of a fixed size. The ATM cells are relatively small compared to those used with older technologies so the small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data dominates the line.

authentication server — A server hosting the accounts database for a RADIUS design.

Automatic Private IP Addressing (APIPA) — A feature of the Microsoft TCP/IP stack since Windows 98. With APIPA, when a client configured to receive its address automatically does not receive a response from a DHCP server, it will use an address in a special range reserved by Microsoft for use with APIPA. This range is 169.254.0.1 to 169.254.255.254 with a subnet mask of 255.255.0.0. The client will select a number from this range, broadcast it on the subnet to ensure that it is not already in use, and keep it until a DHCP server can be located and a new address leased.

Autonomous System (AS) — A group of routers on directly connected network segments that exchange routing information by using a common Interior Gateway Protocol, such as a system in which all OSPF routers in the internetwork are included, with all OSPF routers on directly connected network segments.

availability — The presence of a network service to provide supported services when needed. To provide a high level of availability (as in 24 hours a day, 7 days a week), there must be some redundancy built in.

B2B — A corporate Internet presence that allows companies to transact business or share information with each other.

B2C — An e-commerce or informational site that is used by consumers.

bandwidth — The amount of data that can be transmitted in a fixed amount of time, usually expressed in Kbps or Mbps.

bandwidth throttling — A condition or configuration that limits the rate of transmission, usually described in Kbps or Mbps.

baseband — In network communications, baseband media can carry only one signal at a time.

bastion hosts — A gateway between an inside network and an outside network designed to defend against attacks aimed at the inside network.

batch-oriented processing systems — A computing methodology where work is queued and several units of work are processed at a time. This is easy to program and configure, but it imposes artificial delays.

bindery — The name given to the database used by NetWare 3.*x* to hold user accounts and related information.

bindings — Define the relationships between networking software components. By default TCP/IP, NetBEUI, and NWLink, if installed, are bound to all network interface drivers.

blackhole service — Compiles lists of servers known to originate spam.

Blowfish — A fast, free encryption scheme. For more information, visit *www.counterpane.com/blowfish.html*.

branch deployment model — SNA design model where SNA servers are placed at satellite or branch offices.

bridge — A Data Link layer network device that physically segments a network using the same access method, but that allows the segments to appear as one segment to Network layer protocols.

broadcast — In a TCP/IP network, a traffic type, sent from a single host, in which the destination address of a packet is a special broadcast address. Every device that sees this broadcast packet will process it up through the protocol layers.

brute force — A method of solving a problem by trying all possible combinations as quickly as possible, instead of using reverse engineering.

centralized data collection — Data is gathered at a central point, although it still can be collected from a variety of servers and network devices.

centralized deployment model — SNA design model where SNA servers are located at the same location as the IBM systems.

Channel Service Unit/Data Service Unit (CSU/DSU) — The hardware device used to connect a network to a T-1 or T-3 line.

circuit-level gateway — A session-layer protocol that uses rules to control internal traffic leaving the protected network.

Classless Inter-Domain Routing (CIDR) — A method of public IP addressing allocation that replaces the older system based on classes A, B, and C. CIDR was created to slow down the rapid depletion of public IP addresses, by allocating addresses with more flexible sizes of the ranges of addresses allocated.

Client for NFS — Allows Windows 2000 system users to access files on UNIX NFS systems.

Client Services for NetWare (CSNW) — Microsoft's version of a client used to access NetWare systems.

cloud — Jargon used to describe a network where a given packet could take one of several paths to get to the destination.

codecs (short for *co*mpressor/*dec*ompressor) — Translate audio or video from analog waves that humans hear into electronic signals.

cold spare — A device that is not currently in service but that can be manually placed in service to replace an identical device in the event of a failure.

computationally secure — A method of encryption that is more expensive to break than the encrypted data is worth or that takes so long to break that the data would be worthless by the time it was broken.

context — Name of the container in an NDS database where the object in question resides.

convergence — The point at which the databases of all replication partners match.

cookie — A small file that is used to track user information and state, which is stored on client computers by Web browsers.

counter logs — Track performance data when you need sampled data from performance objects or counters over time. The data is sent to the Performance Logs and Alerts service.

Data Encryption Scheme (DES) — A common 56-bit encryption scheme. For more information, visit *www.itl.nist.gov/fipspubs/fip46-2.htm*.

Data Link layer — Protocols at this layer of the OSI model create, transmit, and receive frames. This layer uses physical addresses. The layer is actually divided into two sublayers: the Logical Link Control sublayer and the Media Access Control sublayer.

decentralized data collection — Data is gathered at multiple places distributed throughout the network.

default gateway — The address of a router on a local network.

delegation of authority — What occurs when upper management delegates specific fiscal or management authority to lower-level personnel, empowering them to act without consulting upper management.

demand-dial connection — A physical connection, such as a circuit-switch WAN link, that is initiated when a router receives packets to be forwarded to a destination across the WAN link.

demand-dial interface — The software component that recognizes the demand-dial connection on behalf of RRAS.

demilitarized zone (DMZ) — A screened subnet between firewalls.

Denial of Service (DoS) — A security attack that prevents the use of a service.

Dfs link — Defined on a Dfs root and appearing to users as a folder below the Dfs root, it is a pointer to a share on that server or another server. It can also point to another Dfs root.

Dfs namespace — The logical view of shared resources as seen by users from Dfs client computers.

Dfs replication — Replication of the root files and folders between root replicas or between Dfs link replicas. Replication is provided by the Windows 2000 File Replication Service (FRS), which is supported only in domain-based Dfs.

Dfs root — The logical starting point of a Dfs hierarchy, hosted on a server.

Dfs shared folder — A folder in the Dfs namespace that is shared by users with proper permission. Sharing of Dfs root-level folders is supported only in domain-based Dfs, but a share can be referred to by Dfs links in both types of Dfs.

Dfs topology — The logical hierarchy of a Dfs, including the roots, links, shared folders, and replica sets, as depicted in the Dfs administrative console.

dial-on-demand (DOD) — An alternate term sometimes used instead of "demand-dial" in Microsoft documentation.

digital certificates — An electronic file that confirms an identity Specified in X.509, it contains a name, serial number, expiration date, and the public key to be used for encryption.

digital signatures — A method of identifying a message that provides nonrepudiation.

Distributed File System (Dfs) — A distributed file management system that creates a unified namespace for users, although the folders of the namespace may reside on many different servers on the network. Users of Dfs simply see a share on a server with a folder hierarchy beneath it. It does not look any different to the user than an ordinary share with disk folders beneath it.

distributed caching — Allows you to distribute a cache across multiple proxy servers.

distributed deployment model — SNA design model that is a combination of the branch and centralized deployment models.

DoD Model — A four-layer model of protocols roughly combining some of the OSI reference model layers in this model. The layers are Process/Application, Host-to-Host, Internet, and Network Access.

Domain Dfs root — In a domain Dfs root, the topology is stored in Active Directory and there can be multiple Dfs root servers, all required to be either domain controllers or member servers in the domain. This is in contrast to a standalone Dfs root in which the topology is stored in the registry of the Dfs root server.

domain filters — Filters that work at the Application layer to allow or deny access to Internet sites based on IP address/subnet mask or domain name.

domain-naming master — A forest-wide single master operations role that is automatically assigned to the first domain controller in the first domain in the forest. The domain-naming master manages the addition and subtraction of domains in the forest.

down-level Dfs client — A computer running an operating system previous to the current operating system and running the Dfs client appropriate to that operating system.

dual-home — A network that has multiple connections to the Internet or a server that has multiple connections (NICs) to a network.

Dynamic Host Configuration Protocol (DHCP) — An Internet protocol that allows computers to receive their IP address and configuration over the network from DHCP servers.

Electronic Data Interchange (EDI) — A standard format for exchanging business data. The standard is ANSI X12.

enterprise application — Any of the mission-critical programs that run your business.

Escon — A channel-based, Data Link layer technology used by IBM mainframes.

Ethernet loop — A condition where frames in an Ethernet are endlessly forwarded in circles.

event-driven — A computing methodology where events can be defined, and those events can act as triggers to initiate responses.

Exchange 2000 — The Active Directory-integrated version of the Microsoft electronic messaging server, introduced in October 2000.

explicit query — A query of Active Directory in which you explicitly and knowingly initiate a search.

Extended Binary-Coded Decimal Interchange Code (EBCDIC) — A binary code for alphabetic and numeric characters that IBM developed for its OS/390 operating system.

extranet — Refers to an intranet that is partially accessible to authorized outsiders. Although an

intranet usually resides behind a firewall and is accessible only to members of the same organization, an extranet allows various levels of accessibility to outsiders if they have a valid user name and password; their identity determines which parts of the extranet they can view. Extranets are becoming a popular means for business partners to exchange information.

failover — In a server cluster, a method by which a server automatically takes over for a failed server.

File and Print Services for NetWare (FPNW) — One of the Windows 2000 services for NetWare that emulates a NetWare 3.*x* server.

File Replication Service (FRS) — A replication service available on Windows 2000 servers in an Active Directory domain. This service replaces the LMRepl service of Windows NT. FRS works only on NTFS volumes, and can be used only in conjunction with other services, such as Active Directory and Dfs.

File Transfer Protocol (FTP) — Both a protocol and its companion service that make file transfer possible between computers using TCP/IP.

firewall — Used to protect a network from unauthorized access and from attacks from another network. A firewall controls traffic in both directions and consists of both hardware and software.

floating single master operations (FSMOs) — The original term used for single master operations. This term is still used in documentation and in tools that let you move the roles, such as the utility NTDSUTIL.

floods — Occur when a switch sends a frame out all ports except the port on which the frame arrived. This usually happens when the switch does not have an entry for the destination MAC address in its forwarding database.

forest — A forest consists of one or more trees, each of which contains one or more domains that share the same schema, configuration, and global catalog.

forwarding database (FDB) — A database in layer 2 devices that matches a port with a MAC address. Used to determine where to send frames.

frame — A packet of transmitted information.

full-duplex — Refers to the transmission of data in two directions simultaneously. For example, a telephone is a full-duplex device because both parties can talk at once. In contrast, a walkie-talkie is a half-duplex device because only one party can transmit at a time.

functionality — The basic requirement of a service, such as file and print sharing, remote access, and WAN connectivity. Meeting the functionality criteria does not indicate that a service is properly configured for availability, security, or performance.

gateway — Software that converts one protocol to another protocol.

Gateway for NFS — Directories on UNIX NFS systems that appear as Windows 2000 shares.

Gateway Services for NetWare (GSNW) — Software that runs on a Windows 2000 server and that allows Microsoft clients access to Novell-managed services.

global catalog server — A special role for one or more domain controllers in a Windows 2000 Active Directory domain. The global catalog server contains a partial replica of every domain directory partition in the forest as well as a full replica of its own domain directory partition and the schema and configuration of directory partitions. This global catalog contains a replica of every object in Active Directory, but only a subset of the attributes of each object. In a multiple domain forest with multiple sites, a global catalog server is required for domain logon by anyone but domain administrators.

hop count — A metric used in routing that indicates the number of routers that a packet must traverse in a certain route.

hosts — A name commonly used to refer to computers in a TCP/IP network.

hot spare — A device that is configured to assume the responsibility of an identical device with no human intervention.

Hot-Standby Router Protocol (HSRP) — A protocol for IP gateway failover specified in RFC 2281 but primarily used by Cisco.

hub — A network device that operates at the Physical layer, serving as both a signal repeater and a central connection point for several network devices.

IAS log file — The file that holds the accounting information on a Windows 2000 IAS server.

in-band data collection — Occurs when status data collected at a decentralized location travels to the centralized collection point over the same network that is running the services and providing access to users. This has a negative impact on the network you are trying to monitor and can yield inaccurate data.

in-band management — Describes a condition when the traffic in question is configured to use the same connection as other data traffic.

infrastructure master — Responsible for keeping track of updates of group-to-user references, such as a renaming of a user account when group memberships are changed in different domains. The infrastructure master in the group's domain registers the updates and replicates them to other infrastructure masters.

integrated services digital network (ISDN) — A standard for telecommunications that includes the ability to transmit voice, data, and video signals over the same media.

Inter-Switch Link (ISL) — A Cisco proprietary specification for VLAN tagging.

Internet — The worldwide network made up of many interconnected networks utilizing public communications lines and the TCP/IP protocol suite.

Internet Control Message Protocol (ICMP) — A protocol by which a host can discover a router automatically, in spite of not having a default gateway configured in its TCP/IP properties.

Internet Security Association Key Management Protocol (ISAKMP) — An IPSec protocol that provides the method by which two computers can agree on a common set of security settings. It also provides a secure way for them to exchange a set of encryption keys to use for their communication.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) — A communication protocol developed by Novell that is necessary for proper communication between NetWare 2.*x*, 3.*x*, and 4.*x* servers.

intranet — A private network that makes information and services available using Internet technologies, such as web servers, web browsers, FTP servers, e-mail, and newsgroups.

intrusion detection — An ISA improvement that monitors activity that would indicate possible hacking.

IP multicast — A technology that allows a one-to-many connection at the Network layer, so that many clients can receive a transmission without requiring the sender to send a packet to each of them.

IP Security (IPSec) — A set of standards developed by the IETF for the next version of IP — IPv6 — and as an optional extension to IPv4. It is included in Windows 2000. IPSec allows for authentication of the source and destination hosts before data is sent. It also allows for the encryption of the data packets during transmission.

Iron Triangle — A metaphor to remind one that the three sides of the triangle, (load, resources, and performance) are related to each other. If load is high and resources are low, performance will suffer. If load is high and performance must be high, the load must be reduced or resources must be increased.

isochronous — Used to describe communications methods that depend on delivery within a specific time period. Data streams, such as multimedia, require an isochronous transport method so that data are delivered as fast as they are displayed and the audio is synchronized with the video.

jitter — The period frequency displacement of a signal from its ideal location.

Korn shell — One type of command line interface environment used on UNIX systems.

latency — The amount of time it takes data to travel from source to destination.

Layer 2 Tunneling Protocol (L2TP) — A protocol based on Cisco's Layer 2 Forwarding protocol and PPTP. It is used to create an encrypted, authenticated tunnel and requires IPSec for encryption.

lease — The period of time for which DHCP clients receive and hold their DHCP address and configuration information.

link replica — One of two or more shares pointing to the same link.

link-state — An algorithm used by the Open Shortest Path First (OSPF) routing protocol in which routers send information to other routers about their direct links. Each router then calculates routes based on this information learned from other routers.

Local Address Table (LAT) — A list of internal subnet addresses maintained by the proxy server, which is actually the routing table of Proxy Server 2.0.

local area network (LAN) — A computer network at its simplest consists of a group of two or more computers linked together to communicate and share network resources, such as files, programs, or printers. In a LAN, networked computers are physically close to one another, often in the same building or on the same office campus.

Logical Link Control (LLC) — A sublayer at the top of the Data Link layer, defined in IEEE 802.2. Includes flow control and management of connection errors.

login scripts — Commands and/or settings executed when an account logs into the NetWare environment.

MAC address — A unique address contained in ROM on every network interface device.

Media Access Control (MAC) — A sublayer of the OSI Data Link layer.

metropolitan area network (MAN) — Connected LANs that span a city or metropolitan area.

Microsoft Directory Synchronization Services (MSDSS) — Collection of tools for integrating and/or migrating NDS and AD.

Microsoft Point-to-Point Encryption (MPPE) — The encryption protocol used with PPTP that includes either 40-bit or 128-bit encryption.

Microsoft SNA Server — Service that provides connectivity between IBM mainframes and Windows 2000.

Microsoft User Authentication Module (MS-UAM) — Allows the Macintosh system to log on to a Windows 2000 environment through the same security that measures a Windows 2000 client encounters when logging on to a Windows 2000 system.

mobile worker — A person who performs his or her work from various locations, using a computer to access resources on the company network, send and receive corporate e-mail, and to transmit data to company servers.

mounted — UNIX term referring to online accessible storage devices.

multicast — A TCP/IP network traffic type in which the packets are addressed to a special group of hosts, defined as a multicast group.

NetMeeting — Software that provides real-time network-based conferencing, including multipoint data conferencing, text chat, whiteboard, and file transfer, as well as point-to-point audio and video.

Network Address Translation (NAT) — An Internet standard that enables a LAN to use one

set of IP addresses for internal traffic and that translates the internal addresses to a second set of addresses for access to an external traffic network (usually the Internet).

Network File System (NFS) — Service on a UNIX machine for accessing files remotely.

Network layer — The layer 3 protocol of the OSI reference model; provides the logical addressing scheme for the network, uniquely identifying devices across the network.

Network Load Balancing (NLB) — A Microsoft product included in Windows 2000 Advanced Server that allows multiple servers to respond to requests in a way that is transparent to the user.

Network Virtual Terminal (NVT) — A protocol used by Telnet sessions so that both ends of the connection can understand each other properly.

network media — The physical cables linking computers in a network.

news server — A server hosting a newsgroup application.

newsgroup — An Internet application that allows users to connect to a server (news server) and read and post articles.

nonrepudiation — Occurs when someone sends you a message (a transaction, for instance) and you can prove that they sent it.

Novell Client for Windows NT/2000 — Client software developed by Novell to access NetWare-managed resources.

Novell Directory Services (NDS) — A directory service developed by Novell and used in NetWare 4.*x* and higher.

NTGATEWAY — A NetWare group required to install and use Gateway Services for NetWare.

NWLink — Microsoft's implementation of Novell's IPX/SPX protocol.

Oakley — A key determination protocol of IPSec that uses the Diffie-Hellman key exchange algorithm.

Open Shortest Path First (OSPF) — A routing protocol support by Windows 2000 that is preferred over RIP for larger networks. OSPF works best in a hierarchically designed network.

Open Systems Interconnect (OSI) reference model — A theoretical model, created many years ago by the International Organization for Standardization (ISO), which defines a layered network model in that protocols at each layer have a defined set of responsibilities in network communications between hosts.

out-of-band data collection — Status data travels through a separate network connection from the one that is running the services and providing access to users. This kind of data collection minimizes the impact of the network analysis itself on the network that you are trying to monitor.

out-of-band management — A condition when the traffic in question is configured to use a dedicated connection so as not to interfere with other data traffic.

outsourcing — The term given to the process of contracting with an outside organization to provide some or all of IT or network infrastructure support and/or personnel.

Packet Internet Groper (PING) — A TCP/IP utility used to test connectivity. It sends packets to addresses, using the ICMP echo request, requesting that the packets be echoed back to the source.

packet filtering — The act of accepting or rejecting IP packets based on a set of rules.

packets — A message is usually broken down into these smaller pieces for easier transmission over a network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

packet switching — A common communications method that divides messages into packets and that sends each packet individually. Each packet

may take different routes and may arrive at the destination out of order. The Internet is based on a packet-switching protocol, TCP/IP. Packet switching differs from circuit switching (the most common communications method), in which a dedicated circuit or channel is established for the duration of a transmission. The best-known circuit-switching network is the telephone system, which links wire or fiber-optic segments to create a single unbroken line for each telephone call. Circuit-switching systems are best when data must be transmitted in real time. Packet-switching networks are more efficient if some amount of delay is acceptable.

Partition Knowledge Table (PKT) — A table that maps links and shares for the Dfs namespace.

passive caching — When active caching is disabled, the proxy cache service retrieves Web pages only when clients request them.

Password Authentication Protocol (PAP) — An Internet standard plain text authentication scheme included in Windows 2000 to allow clients to connect to non-Windows 2000 remote access servers and to allow non-Windows clients to connect to Windows RAS servers.

password synchronization — Permits users to use the same synchronized password for Windows and UNIX systems.

PDC emulator — In a mixed-mode domain, the PDC emulator "pretends" to be a Windows NT 4.0 PDC to replicate directory changes to the BDCs in the domain. In a native-mode domain, the PDC emulator also receives preferential replication of password changes from other Windows 2000 domain controllers.

Performance Logs and Alerts — A new service of Windows 2000 that allows administrators to gather data for analysis and to be alerted when predefined events occur or when thresholds are exceeded.

performance — A measurement of the operation, function, and effectiveness of a service that is often related to how fast things happen.

Physical layer — The bottom layer of the OSI reference model. It includes the media that carries the signals and the physical devices for network connection and control.

Point-to-Point Protocol (PPP) — A standard method for encapsulation of point-to-point network traffic that defines packet boundaries, identifies the protocol of the encapsulated packet, and includes bit-level integrity services.

Point-to-Point Tunneling Protocol (PPTP) — An Internet-layer protocol that encapsulates PPP frames within IP datagrams to be transmitted over an IP internetwork.

point-to-point — A connection between two locations using a communications carrier's network.

port — An identifier used in a TCP/IP packet to determine the program or service that is sending or receiving data. Ports are associated with protocols, such as TCP or UDP. For instance, TCP port 20 identifies File Transfer Protocol (FTP) data.

port mirroring — A common industry term used to describe a configuration that sends copies of frames from one or more ports to a designated port. Used for protocol analyzers, RMON devices, and so on.

port spanning — A Cisco term used to describe a configuration that sends copies of frames from one or more ports to a designated port. Used for protocol analyzers, RMON devices, and so on.

Post Office Protocol (POP) — A protocol used to send and retrieve e-mail from a mail server. Most e-mail applications use the POP protocol, although some can use the newer Internet Message Access Protocol (IMAP). There are two versions of POP in use today. The first, called POP2, became a standard in the mid-80s and

requires SMTP to send messages. The newer version, POP3, can be used with or without SMTP.

Presentation layer — The Presentation layer of the OSI reference model is where formatting of the data, and any necessary data conversion, is done. In addition, it handles data compression, data encryption, and data stream redirection.

proof-of-concept — A scaled-down version of an entire project.

protocol — In networking, this is a set of rules for communicating between systems.

protocol stack — A logical layering of protocols, as defined in the OSI reference model and the DoD model.

proxy array — Two or more proxy servers that function in parallel to provide the caching service. A proxy array appears as one machine to the client; each server contains separate cached data. A proxy array provides a load-balancing function for Web caching. If one server becomes unavailable, the other servers continue to function.

proxy chains — A group of servers or arrays that work in a hierarchical structure. One server receives a request and, if it does not have the information associated with a URL cached locally, sends the request up the chain to the next "upstream" server.

proxy server — A server hosting proxy services.

proxy service — An Application-layer gateway service that makes network connections for internal client computers and that isolates a private network from an external network (most commonly the Internet). Conversely, a proxy server may restrict inbound traffic when performing reverse proxy functions.

public addresses — Addresses assigned to an organization by an ISP or ARIN.

publisher — Term used by Microsoft to refer to Active Directory when migrating directory data from NetWare to Windows 2000.

pull partner — Requests data to be sent to it from other WINS servers.

push partner — Sends data to other WINS servers based on the number of changes to the database.

push/pull partner — Requests changes from partners at an interval and pushes changes to partners when there are changes to the database.

Quality of Service (QoS) — A name for a set of components by which Windows 2000 provides bandwidth reservation capability.

Quality of Service (QoS) — A networking term that specifies a guaranteed throughput level.

RADIUS server — The server that accepts authentication requests from a RADIUS client and authenticates the user accounts with an authenticating server.

realm — The entity containing the information for authentication (more global than authentication server).

redundancy — Removing a "single point of failure" for one component or class of components to provide fault tolerance redundancy. In networking, having multiple servers offer the same service can provide redundancy, and multiple routers can give access to the same subnet.

referral — In Dfs for Windows 2000, it is information presented to a Dfs client attempting to gain access to a portion of the Dfs namespace. The referral contains a mapping of a DNS name to the UNC of the share associated with that portion of the Dfs topology.

relay agent — A computer that listens for DHCP/BOOTP traffic on a subnet.

remote access — A network model that allows users located physically at a distance from the network to access the network, using either a dial-in connection or a virtual private network (VPN) connection.

remote access client — Dials in to a remote access server.

remote access policies — A set of conditions and connection settings used to grant remote access. Remote access policies are made up of many simple parts grouped into three components: conditions, permissions, and profile.

Remote Authentication Dial-in User Service (RADIUS) — An industry standard that offers centralized authentication of ISP or private remote access users. It is a security enhancement that also provides centralized accounting of dial-in connections.

remote office — A network model that describes a network designed to connect one or more remote segments of the organization with the organization's network. This model could involve using technologies associated with other models.

Remote Procedure Call (RPC) — Protocol used to exchange messages between machines.

resolver — A DNS client computer, which sends requests to DNS servers in order to resolve DNS names to IP addresses.

reverse proxy — A service that allows a proxy server to respond to all user requests on behalf of the actual server.

RID master — Allocates new relative IDs that are used together with the domain security ID (SID) to create unique security IDs for each object that can be a security principle.

RMON (Remote Monitoring) probe — A subset of the SNMP protocol that provides history, statistics, alarms, and so on for network traffic.

RMON — Short for Remote Monitoring, a protocol that allows the monitoring of RMON-enabled hubs and switches from a workstation.

root replica — A duplicate of a Dfs root on another server, it provides greater availability because a root server is responsible for providing referrals to clients for shared folders. If a root server becomes unavailable and a root replica has not been created, the Dfs namespace becomes inoperative.

router — A Network layer device that connects segments, transmitting packets between segments based on the logical (Network layer) network address. Routers have their own specialized protocols that aid in selecting the best path for packets to travel.

Routing Information Protocol (RIP) — A simple routing protocol for small internetworks of less than 16 subnets. Windows 2000 supports RIP version 2 for IP and IPX protocols, but has a limit of 15 subnets.

rules — Parameters by which traffic is allowed or disallowed by a filtering or proxy service.

SAP Agent — Service running on the Windows 2000 system responding to queries from clients such as Get Nearest Server.

scalability — The ability of a computer or network to respond to increased demands.

schema master — Every domain controller in the forest has a copy of the schema for Active Directory, but only the schema master has a writeable copy. By default, the first domain controller in the first domain in the forest has this role, but this role can be transferred to another domain controller in the forest as needed.

scope — A contiguous range of addresses for a single subnet.

screened subnet — A network that is exposed to another organization but partially protected by a firewall.

security — Something that gives or assures safety. In networking, this can include the authentication process and various methods of security access to individual network resources. The term also applies to the strength of security applied and the methods used.

security — Security as applied to networks has many meanings. These include privacy, which means other people can't see your data; integrity, which means other people can't change your data; authentication, which means you know someone is who they say they are; nonrepudiation, which means that when someone completes a transaction, they can't go back and claim it never happened; and prevention of denial of service.

security association (SA) — The combination of the security method agreed upon and the keys the method uses.

security token — A device that provides a special key required to log on to a system.

segment — A physical portion of a network.

Serial Line Internet Protocol (SLIP) — The predecessor protocol to PPP for sending IP packets over a serial connection.

Server for NFS — Windows directories appear as NFS file systems.

Server for NIS — Allows a Windows 2000 server to operate as a NIS server and to integrate with other NIS servers and domains.

Server for PCNFS — Allows Windows systems running NFS Client to authenticate to UNIX systems.

server roles — The functions assigned to servers, such as file and print, applications, WINS, and DNS.

Service Advertising Protocol (SAP) — Used by IPX/SPX services to make known their identity and services.

Services for Macintosh — Provides a mechanism for Windows 2000 systems to access Macintosh network services using TCP/IP or AppleTalk.

Services for NetWare (SFN) v. 5 — Designed for integrating Windows 2000 server systems into an existing NetWare environment.

services — Software components that provide certain functionalities. Accessing this functionality often depends on a client component. For instance, the DHCP service provides automatic IP configuration to a computer configured to be a DHCP client. Microsoft Internet Information Services allows administrators to publish web pages that are accessible when users connect to the IIS server with an Internet browser, such as Internet Explorer.

session — A logical connection between Active Directory and Novell Directory Services.

Session layer — The Session layer of the OSI reference model manages the session between two computers, working to establish, synchronize, maintain, and end each session. Authentication, connection identification, data transfer, acknowledgments, and connection release are performed by the protocols at this layer.

shared secret — A text string that serves as a password between the RADIUS server and the RADIUS clients connected to it.

single master operation roles — Roles for Active Directory domain controllers. Roles include the schema master, the domain-naming master, the RID master, the PDC emulator, and the infrastructure master.

single point-of-failure — A physical or logical object in a system whose failure will cause the entire system to fail.

Socks proxy — An application-layer gateway, often considered a generic proxy, which can be used with virtually any TCP application, including Web browsers and FTP clients. Often used for services that do not have their own application proxy. In this case, the Socks proxy intercepts the packets and regenerates the packet while placing the original payload within the new packet.

spam — Unsolicited or unwanted e-mail messages.

Spanning Tree Protocol (STP) — An IBM protocol adopted by IEEE that configures a group of switches to prevent loops.

spoofing — In firewalls, this term applies to the replacement of the source address in the IP header with an address that is allowed by the firewall.

standalone Dfs root — Windows 2000 supports the standalone Dfs root supported by Windows NT 4.0, in which the Dfs root is hosted on a single computer and the Dfs topology is stored on that computer.

state — Maintaining information about a user during a visit to a Web site or maintaining information about a stream of data in the network.

stateful packet filtering (also stateful inspection) — This type of filtering maintains state information on current connections, which enables it to determine when a return connection applies to a connection established from within the network. If a return connection does not have its origins from the private network, it may be part of a hacking attempt, such as a denial of service.

stateless packet filtering — This type of filtering does not retain connection information and just makes forward/drop decisions based on packet header information.

steganography — The practice of concealing a message.

sticky connection — When traffic directors send all packets from a single source to a single destination.

strong authentication — An authentication scheme that combines multiple schemes, typically requiring a user name, password, and either a token or certificate.

stub area — An OSPF area that does not advertise individual external networks. It is a portion of a network with a single entry and exit point that does not maintain routes to external Autonomous Systems.

subnetting — The act of taking a network address, such as 192.168.0.0/16, and borrowing bits from the host portion to subdivide this single network address into multiple network addresses.

subscriber — Term used by Microsoft to refer to the NetWare system when migrating files from NetWare to Windows 2000.

supernetting — Borrowing bits from the network portion to combine several network addresses into one.

switch — A device that combines the capabilities of a hub and a bridge, going beyond the multiport repeater capabilities of a hub by routing based on MAC address.

synchronous — Usually used to describe communications in which data streams can be delivered only at specific regular intervals.

Synchronous Optical NETwork (SONET) — A high-speed Physical-layer protocol standard for MAN technology using fiber-optic cable.

System Monitor — A tool, found in the Performance console, to use when you want to immediately see real-time performance, produce reports on monitored data, and/or view performance logs that you create using Performance Logs and Alerts. System Monitor works with objects, instances of objects, and counters of each object.

Systems Network Architecture (SNA) — An architecture created by IBM for communications between hosts.

Systems Network Architecture (SNA) — Communication protocol developed by IBM.

T-carrier system — A system developed by Bell Telephone Laboratories to multiplex voice signals onto digital transmission lines. Customers buy all or a portion of the T-carrier capabilities. The levels of service include T-1 at 1.544 Mbps and fractional T-1 that provides a portion of the T-1 bandwidth.

Telnet client — Connects to ands run applications on a Telnet server.

Telnet server — Allows systems using Telnet access to the Windows 2000 server.

Time Division Multiple Access (TDMA) — A multiplexing method used on SONET networks that divides broadband communications channels into separate time slots in order to allow more data to be carried simultaneously.

Time to Live (TTL) — When a Dfs client gains access to a shared folder in the Dfs namespace, it caches that portion of the table for the length of time specified in the TTL attribute for the root share or link share.

Token Ring network — A physical star but logical ring network standard developed by IBM, using the token-passing access method.

tombstoning — Marking something in a database to eventually be deleted.

topology — The physical layout of transmission media and the logical method for transmitting data, mapping to the Physical and, usually, Data Link layers of the OSI reference model.

total cost of ownership (TCO) — A term to remind people that the implementation cost of a system is only one part of the total cost. To appreciate what a system really costs, you have to include the design and implementation cost, the ongoing updates of the system, the training of administrators and users, regular maintenance of the system across time, and technical support required to keep the system going.

trace logs — Track performance data associated with events such as disk and file I/O, network I/O, page faults, or thread activity. The event itself triggers the performance data to be sent to the Performance Logs and Alerts service.

Transmission Control Protocol/Internet Protocol (TCP/IP) — A widely used protocol suite for routed networks, which includes many more protocols than the two used to identify it.

Transmission Control Protocol/Internet Protocol (TCP/IP) — Communication protocol used on the Internet. It is commonly found on large networks.

transparent query — A search of Active Directory initiated by an action of the user. The user may not be aware that the action, such as domain logon, initiated an Active Directory search.

Transport layer — The Transport layer of the OSI reference model is responsible for error and flow tracking, dividing outgoing messages into smaller segments, and reassembling incoming messages.

transport mode — The mode in which IPSec can be used to authenticate and/or encrypt communications between computers without using a tunnel.

tree — Name of an NDS database.

Triple DES — An encryption scheme similar to DES that uses 128 bits.

Trojan horse virus — A virus disguised as a benign program.

tunnel mode — The mode in which IPSec will encapsulate IP packets and optionally encrypt them.

unconditionally secure — An encryption scheme that cannot be broken because the information required to unlock the encryption is not transmitted with the message.

unicast — In a TCP/IP network, a unicast packet is addressed to a single host.

variable-length subnet masks (VLSMs) — Used to produce subnets of different size from a single network address.

Virtual Router Redundancy Protocol (VRRP) — An open protocol for IP gateway failover used by many vendors.

virtual links — If a router designated as an ABR does not have a direct physical connection to the backbone, a virtual link can be created through an area that is connected to the backbone. This only results from poor design, or as part of a temporary work-around during changes to the network. A linkage occurs when two routers belong to the same area but are not physically connected to the same backbone area.

virtual private network (VPN) — The encapsulation or "tunneling" of packets between end points over a network for security.

VLAN Trunking — A network configuration that allows traffic from multiple VLANs to be transmitted and received on the same interface. Used to conserve expensive uplink ports.

Web caching — Proxy Server 2.0 caches Web pages it retrieves on the behalf of clients. It then checks its cache before retrieving the data on subsequent queries from clients. If the data is in the cache, Proxy Server 2.0 provides it from the cache.

Web proxy — An application-layer gateway service that stands in for outbound connection attempts by Web browser clients, making the request to the Web server on behalf of the client and hiding the actual address of the Internal client.

web browser — The client software of the World Wide Web that allows users to browse for Web servers and display the content.

web servers — The servers, located on an intranet or the Internet, that provide graphical content accessed by client computers using special web browser software that can interpret and display the content.

wide area network (WAN) — A network of networks connected across large geographical areas, even spanning continents and oceans.

Windows clustering — The use of multiple physical computers to provide a service that appears to be hosted on just one server.

WinSock proxy — An application layer gateway service that is available to clients with the WinSock proxy client installed. The WinSock proxy client can support any protocol that uses WINSock.DLL, including FTP, NNTP, Telnet, SMTP, POP3, RealAudio, HTTP, and HTTPS.

zone — A contiguous portion of the Domain Name Space.